(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 827 329 A1

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
04.03.1998 Bulletin 1998/10

(51) Int Cl.6: H04N 1/32, G06K 9/00

(21) Application number: 97306278.9

(22) Date of filing: 19.08.1997

(84) Designated Contracting States:
AT BE CH DE DK ES FI FR GB GR IE IT LI LU MC NL PT SE
Designated Extension States:
AL LT LV RO SI

(30) Priority: 29.08.1996 US 697753

(71) Applicant: LUCENT TECHNOLOGIES INC.
Murray Hill, New Jersey 07974-0636 (US)

(72) Inventor: Wilfong, Gordon Thomas
Gillette, New Jersey 07933 (US)

(74) Representative:
Watts, Christopher Malcolm Kelway, Dr. et al
Lucent Technologies (UK) Ltd,
5 Mornington Road
Woodford Green Essex IG8 OTU (GB)

(54) Validation stamps for electronic signatures

(57) The present invention describes a validation stamp for protecting the integrity of a signature affixed to an electronic document. The validation stamp of the present invention includes a validation body and a validation signature. The validation stamp is affixed to a signed document having a document body and a document signature. The document signature and the validation signature are derived from an electronic signature defined by geometric and timing information. Specifically, the validation signature includes the timing information, and possibly the geometric information, of the electronic signature, whereas the document signature includes the geometric information, and not the timing information, of the electronic signature. To verify the integrity of the signature on the electronic document, the validation signature is first decrypted and then compared, along with the document signature, against the signed document and geometric and timing information of a signature known for the authorized signator of the electronic document.

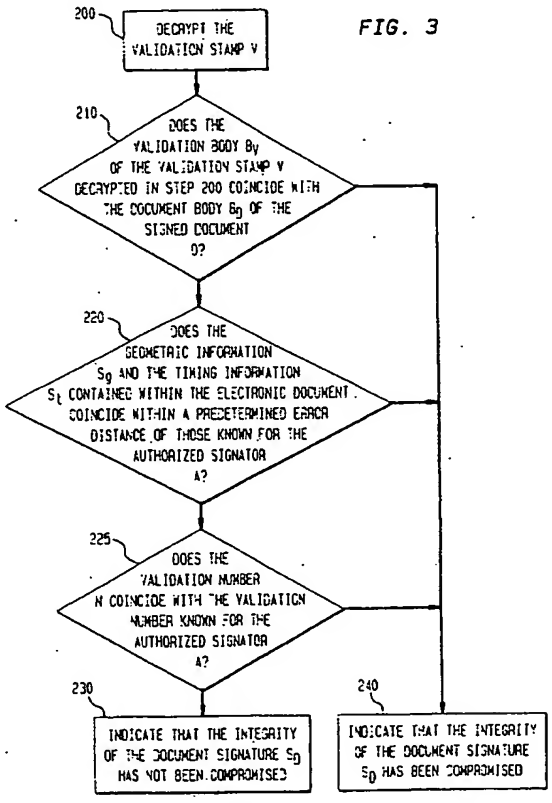


FIG. 3

EP 0 827 329 A1

Description

FIELD OF THE INVENTION

The present invention relates generally to the field of electronic documents and, more particularly, to signature verification on electronic documents.

BACKGROUND OF THE INVENTION

In certain instances, office work productivity has significantly increased through advances in technology. Some of these advances in technology involve replacing paper documents in the workplace with electronic documents. One such advance provides office workers with the ability to send/receive and share documents electronically. Traditionally, many paper documents contain signatures to show authorship or indicate approval. Accordingly, it is also desirable to include signatures in the electronic documents, particularly when they are sent back and forth. As would understood, the inclusion of signatures in the electronic documents is easily achieved using graphic tablets, for example, which are computer peripheral devices for capturing handwritten data.

Once a signature is affixed to a document, people generally assume that the signature on a paper or electronic document is proof of authorship or approval. There is no guarantee, however, that the integrity of the signature, especially electronic ones, has not been compromised, for example, by being traced or otherwise forged. Generally, signatures on paper or electronic documents are vulnerable to two forms of deception. The first form of deception involves an invalid signature. An invalid signature is a signature created by a forger attempting to imitate the signature of another person, i. e., authorized signator. Such a signature is affixed on a document not authored or approved by the authorized signator. The second form of deception involves affixing a valid signature, which is a signature actually created by the authorized signator, on a document other than the original intended document. This form of deception, referred to herein as an invalid copy, is particularly difficult to detect when the signature has been "cut" from one electronic document and "pasted" onto a second electronic document since it looks exactly like the original signature.

For the aforementioned reasons, a number of people have reservations about allowing their signature to be captured electronically. Accordingly, there exists a need for protecting the integrity of a signature on an electronic document.

Summary of the Invention

A validation stamp is provided for protecting the integrity of an electronic signature on a document, wherein said document includes a document body and a document signature, said document signature including geometric information corresponding to said electronic signature, said validation stamp comprising: a validation signature including timing information corresponding to said electronic signature for ensuring that said electronic signature is a valid signature; and a validation body identical to at least a portion of said document body for determining whether said electronic signature was originally intended for said document.

The validation signature may be encrypted such that said timing information is concealed from recipients of said document. The validation signature may be decryptable for comparing said timing information of said validation signature against timing information known for an authorized signator of said electronic signature.

The validation signature may further include said geometric information corresponding to said electronic signature. The validation signature may be decryptable for comparing said timing information and said geometric information of said validation signature against timing information and geometric information known for an authorized signator of said electronic signature. The validation body may be identical to the entire contents of said document body. Alternatively, it may be identical to predetermined portions of said document body.

The validation body may be operable for comparing against said document body.

The validation stamp may further comprise a document signature including geometric information corresponding to said electronic signature which has been modified such that said timing information corresponding to said electronic signature cannot be reconstructed from modified geometric information. The geometric information may be modified such that adjacent points comprised in said modified geometric information are equal arc-length distances from each other. Alternatively, the geometric information may be modified such that a random number of chosen points are interpolated between adjacent points comprised in said geometric information.

A method for protecting an electronic signature affixed to an electronic document comprises the steps of: creating a signed document having a document body and a document signature; and assembling a validation stamp for said signed document, wherein said validation stamp includes a validation signature and a validation body.

The method may comprise the additional step of appending said validation stamp to said signed document, wherein said validation stamp may be referenced to protect the integrity of said electronic signature on said electronic document.

The document signature may include geometric information describing geometric signature features of a signator of said electronic signature. The geometric information may be modified such that timing information corresponding to said geometric information cannot be reconstructed from modified geometric information. The

modified geometric information may include adjacent points which are equal arc-length distances from each other. Alternatively the modified geometric information may include a random number of chosen points interpolated between adjacent points comprised in unmodified geometric information.

The method may include the additional step of: comparing said validation body against said document body to determine whether said electronic signature was originally intended by an authorized signator to be affixed to said electronic document.

The method may include the additional step of: comparing geometric information and timing information contained within said signed document and said validation stamp against geometric information and timing information of a signature known for an authorized signator to determine whether said signature is a valid signature.

The validation signature may include geometric information describing geometric signature features of a signator of said electronic signature and timing information describing dynamic signature features of said signator of said electronic signature.

The method may include the additional step of capturing a signature electronically using a graphics tablet operable to record positions of a writing device on said graphics tablet at given times. The step of creating said signed document may include deriving said document signature using geometric information of said electronic signature being captured electronically by said graphics tablet. The step of creating said signed document may include deriving said validation stamp using timing information of said electronic signature being captured electronically by said graphics tablet.

The method may include the additional step of encoding said validation stamp such that said validation stamp is not accessible to recipients of said electronic document.

The validation body may be identical to said document body such that said validation body may be later compared to said document body for determining whether said electronic signature was originally intended by an authorized signator to be affixed to said electronic document. Alternatively, the validation body may be identical to predetermined portions of said document body such that said validation body may be later compared to said document body for determining whether said electronic signature was originally intended by an authorized signator to be affixed to said electronic document.

The validation signature may include timing information describing dynamic signature features of a signator of said electronic signature.

The validation stamp may include a validation number identifiable with a signator to protect against deception.

A method for verifying the integrity of an electronic signature on an electronic document having a signed document and an encrypted validation stamp, comprises the steps of: decrypting said validation stamp; and comparing said validation stamp being decrypted against said signed document to determine whether said electronic signature was originally intended by an authorized signator to be affixed to said electronic document.

The signed document may include a document body, said validation stamp may include a validation body, and said step of comparing said validation stamp may include comparing said validation body against said document body to determine whether said validation body coincides with said document body.

The signed document may include said document signature, said validation stamp may include a validation signature and said method may include the additional step of comparing timing information of said validation signature and geometric information of said document signature against geometric information and timing information of a signature known for an authorized signator to determine whether said electronic signature is a valid signature.

The validation stamp may include a validation signature and said method may include the additional step of comparing geometric information and timing information of said validation signature against geometric information and timing information of a signature known for an authorized signator to determine whether said electronic signature is a valid signature.

A method for verifying the integrity of an electronic signature on an electronic document having a signed document and an encrypted validation signature, comprises the steps of: decrypting said validation signature; and comparing said validation signature being decrypted against timing information of a signature known for an authorized signator of said signed document to determine whether said validation signature is a valid signature.

The method may include the additional step of comparing said validation signature being decrypted against geometric information of a signature known for an authorized signator of said signed document to determine whether said validation signature is a valid signature.

The signed document may include a document signature and said method may include the additional step of comparing said document signature against geometric information of a signature known for an authorized signator of said signed document to determine whether said validation signature is a valid signature.

The present invention relates to a validation stamp that protects the integrity of a signature affixed to an electronic document. Specifically, the validation stamp protects against deceptions relating to invalid copies and invalid signatures.

In one embodiment, the validation stamp of the present invention protects signed documents comprising a document body and a document signature against invalid copies and invalid signatures. The validation

stamp is encrypted and includes a validation signature and a validation body, which is identical to the document body or portions thereof when created. The document signature and the validation signature are derived from an electronic signature captured using a graphics tablet, wherein the electronic signature is defined by geometric information and timing information. Specifically, the validation signature is derived using the timing information, and possibly the geometric information, associated with the electronic signature, and the document signature is derived using only the geometric information associated with the electronic signature. In a preferred embodiment of the present invention, the geometric information used to derive the document signature is modified such that possible reconstruction of the timing information from the original geometric information is prevented.

The integrity of the signature affixed to the electronic document is verified by decrypting the validation stamp and comparing the decrypted validation stamp and, in some instances, the document signature against the document body and the geometric and timing information associated with a signature known for an authorized signator. Specifically, the validation body is compared to the document body to determine whether the authorized signator originally intended to affix his or her signature to the electronic document, and the geometric information and the timing information contained within the electronic document are compared to the geometric and timing information associated with the signature known for the authorized signator to determine whether the signature on the electronic document is a valid signature. The signed document is a valid copy if the validation body is identical to the document body or predetermined portions thereof. The signature is a valid signature if its geometric and timing information coincide within a predetermined error distance of the geometric and timing information of the signature known for the authorized signator.

BRIEF DESCRIPTION OF THE DRAWINGS

For a better understanding of the present invention, reference may be had to the following description of exemplary embodiments thereof, considered in conjunction with the accompanying drawings, in which:

Fig. 1 illustrates an electronic document *E* comprising a signed document *D* and a validation stamp *V* in accordance with the present invention;

Fig. 2 illustrates a flowchart depicting the steps of an exemplary validation routine for validating the electronic document *E* of Fig. 1;

Fig. 3 illustrates the flowchart of Fig. 3 having an additional step for verifying validation numbers; and

Fig. 4 illustrates one embodiment of a signature verification system in connection with the present invention.

DETAILED DESCRIPTION

The present invention is a validation stamp that protects the integrity of a signature on an electronic document. Specifically, the present invention protects against deceptions relating to invalid copies and invalid signatures, as will be described herein.

Referring to Fig. 1, there is illustrated an electronic document *E* 02 comprising a signed document *D* 04 and a validation stamp *V* 06 in accordance with the present invention, i.e., $E=(D,V)$. As shown in Fig. 1, the signed document *D* 04 is accessible to recipients of the electronic document *E* 02, and includes a document body B_D 10 consisting of textual and/or graphical information and a document signature S_D 08 to indicate authorship or approval of the document body B_D 10, i.e., $D=(S_D, B_D)$.

The validation stamp *V* 06 provides a mechanism for verifying the integrity of the document signature S_D 08 in the signed document D 04, and includes a validation signature S_V 12 and a validation body B_V 14, which is the same as the document body B_D 10. Thus, $V=(S_V, B_V)=(S_V, B_D)$. In an alternate embodiment of the present invention, the validation body B_V 14 contains predetermined portions or segments of the document body B_D 10 in lieu of the entire document body B_D 10.

Unlike the signed document D 04, the validation stamp V 06 is encrypted using an encoding algorithm and is therefore unaccessible to the recipients of the electronic document E 02. Encoding algorithms, such as the Digital Signature Algorithm (DSA) standard, are well-known in the art. See American National Standards Institute (ANSI), "Working Draft X9.30-199X: Public Key Cryptography Using Irreversible Algorithms for the Financial Services Industry: Part I: The Digital Signature Algorithm (DSA)," American Bankers Association, Washington, D.C., March 4, 1993.

The document signature S_D 08 and the validation signature S_V 12 are derived from a signature captured by a device operable to electronically record the positions of a writing device, such as a pen, on the device at given times. Such devices are referred to herein as graphics tablets, and are well-known in the art. As would be understood, the term "graphics tablet" should not be construed to limit the present invention in any manner in that other known methods of electronically capturing a signature may also be utilized. For the purposes of this application, signatures captured electronically using a graphics tablet are referred to herein as "electronic signatures," while signatures written with an ink pen on paper documents or captured electronically by a means other than a graphics tablet are referred to herein as "paper signatures."

Electronic signatures have associated with them two types of information which the present invention utilizes to determine whether the integrity of a signature on an electronic document has been compromised: geometric information S_g and timing information S_t. The

geometric information S_g describes the geometric signature features, i.e., shape of the signature, and is captured by the graphics tablet as a sequence of points $(p_1,...,p_n)$. Each point has (x,y) coordinates.

The timing information S_t defines the moment each of the points $(p_1,...,p_n)$ are recorded electronically by the graphics tablet with reference to each other. Thus, for each point P_i comprising the geometric information S_t of an electronic signature, there is associated a (x_i,y_i) coordinate and a time t_i, i.e., $p_i=(x_i,y_i,t_i)$. The timing information S_t is used to derive dynamic signature features of the signator, such as the motion or speed of a writing device as a signator writes each letter of his or her name on the graphics tablet. The dynamic signature features are not apparent from a copy of the signature.

The geometric information S_g and the timing information S_t play somewhat complementary roles in distinguishing genuine signatures from forgeries, i.e., the more forgers try to match every detail of a signature's shape, the less likely they are to match its dynamic signature features, and vice-versa. In contrast to electronic signatures, paper signatures have associated geometric information S_g only, whereby the absence of the timing information makes such signatures more vulnerable to forgery.

The validation signature S_V 12 is derived using the electronic signature and contains the timing information S_t and possibly the geometric information S_g. In contrast, the document signature S_D 08, which is also derived using the electronic signature S, contains only the geometric information S_g -- that is, the geometric information S_g is isolated or the timing information S_t is removed from the electronic signature in order to create the document signature S_D. Thus, the document signature S_D is equivalent to a paper signature. Since the document signature S_D contains only the geometric information S_g and the validation stamp V 06 is encrypted, the timing information S_t is hidden from the recipients of the electronic document E 02, thereby preventing access to the dynamic signature features for imitation by a forger.

The basic assumption that enables the success of the present invention is that the timing information S_t is concealed. However, this may not be the case, for instance, if the graphics tablet samples the position of the writing device at regular time intervals I_n. In such a situation, the timing information S_t could be easily reconstructed from the geometric information S_g using the formula $t_i=(i-1)*I_n$. In order to hide the timing information S_t and prevent its reconstruction from the geometric information S_g, the geometric information $(p_1,...,p_n)$ is modified before being recorded as the document signature S_D. For example, the document signature S_D could be computed by simply re-sampling the raw geometric information $(p_1,\cdots,p_n)$ to produce modified geometric information $(p_1',...,p_n')$ where adjacent points p_i' are equal arc-length distances from each other. Another example involves interpolating a random number of chosen points between adjacent points of the raw geometric information $(p_1, ..., p_n)$.

In general, signatures on electronic documents are subject to two forms of deception: invalid copy and invalid signature. An invalid copy is a signature that was actually produced by the authorized signator, i.e., valid signature, for a document other than the one on which the signature is currently affixed. In other words, the invalid copy of the signature is not on the document which the authorized signator originally affixed his or her signature. For example, a valid signature may be "cut" from one electronic document and "pasted" onto a second electronic document. The second form of deception, i.e., invalid signature, involves a forger attempting to imitate the geometric and/or dynamic signature features associated with a signature of another person. This signature is also affixed to a document not authored or approved by the authorized signator.

The present invention electronic document E 02 is operable to resist both of the aforementioned forms of deception. In operation, an authorized signator or author A would create the electronic document E and send it to recipients R. The recipients R would have access to the signed document D, but not to the encrypted validation stamp V. To verify that the integrity of the signature on the electronic document was not compromised, the recipients R would run a validation routine which compares the validation body B_V and the geometric information S_g and the timing information S_t contained within the electronic document against the signed document D and the geometric and timing information of a signature known for the author A.

Referring to Fig. 2, there is illustrated a flowchart depicting the steps of an exemplary validation routine 20. As shown in Fig. 2, the validation routine 20, in step 200, decrypts the validation stamp V to access the encrypted validation body B_V and the timing information S_t, and possibly the geometric information S_g, corresponding to the encrypted validation signature S_v. In step 210, the validation routine checks for the first form of deception, i.e., invalid copy, by comparing the decrypted validation body B_V against the document body B_D of the signed document D. If the decrypted validation body B_V coincides with the document body B_D, then the validation routine 20 concludes that the document signature S_D and the validation stamp V was not "cut" from another electronic document E and "pasted" onto the electronic document E received -- that is, the document signature S_D is not an invalid copy. The validation routine 20 subsequently continues to step 220. Otherwise, the validation routine 20 proceeds to step 240 where the recipients R are informed that the integrity of the document signature S_D on the electronic document E received has been compromised.

In step 220, the validation routine 20 checks for the second form of deception, i.e., invalid signature, using a signature verification algorithm to validate the signature on the electronic document. Signature verification

algorithms are well-known in the art. See "Statistical Methods for On-Line Signature Verification" by Winston Nelson, William Turin and Trevor Hastie in the International Journal of Pattern Recognition and Artificial Intelligence, Volume 8, Number 3, 1994. In short, signature verification involves establishing statistical information about a number of features of a given person's signature, such as average time to write a signature, average speed of pen during signing, average number of strokes, etc. This statistical information is typically established during a training phase. To verify a particular instance of a signature, the signature verification algorithm measures the features of interest and statistically tests whether the results are similar within a predetermined error distance, such as Euclidean, to those obtained during the training phase.

In other words, the signature verification algorithm compares the timing information S_t of the decrypted validation signature S_v and the geometric information S_g of the document signature S_D (or decrypted validation signature S_v) against those known for the authorized signator A. If the geometric information S_g and the timing information S_t are similar within the predetermined error distance of the known geometric information S_g and the timing information S_t of the authorized signator, then the decrypted validation signature S_v is determined to be actually produced by the authorized signator A, i.e., valid signature. The validation routine 20 subsequently continues to step 230 where it indicates to the recipients that the integrity of the document signature S_D on the electronic document E received has not been compromised. Otherwise, the validation routine 20 proceeds to step 240 where it indicates that the integrity of the document signature S_D on the electronic document E received has been compromised.

In another embodiment of the present invention, the validation stamp V further includes a validation number N for providing additional protection against invalid signatures, wherein each validation number N comprises a sequence of characters which can be used to uniquely identify a person or other type of entity. Thus, if a forger is able to successfully imitate the geometric and dynamic signature features of another persons's signature, the forger must also know the authorized signator's associated validation number N. Referring to Fig. 3, there is illustrated a flowchart depicting the steps of the validation routine 20 having a step 225 for verifying the validation number N. In an alternate embodiment of the present invention, the validation number N is included in the validation stamp V in lieu of the timing information S_t.

Referring to Fig. 4, there is illustrated one embodiment of a signature verification system 40 in connection with the present invention. As shown in Fig. 4, the electronic signature verification system 40 includes a computing device 42 for creating and verifying the electronic document E 02, a display 44 for providing a visual presentation, a keyboard 46 for providing typed input and a graphics tablet 48 for providing handwritten input. The display 44, the keyboard 46 and the graphics tablet 48 are electronically coupled to the computing means 42.

Claims

1. A validation stamp for protecting the integrity of an electronic signature on a document, wherein said document includes a document body and a document signature, said document signature including geometric information corresponding to said electronic signature, said validation stamp comprising:

   a validation signature including timing information corresponding to said electronic signature for ensuring that said electronic signature is a valid signature; and
   a validation body identical to at least a portion of said document body for determining whether said electronic signature was originally intended for said document.

2. A method for protecting an electronic signature affixed to an electronic document comprising the steps of:

   creating a signed document having a document body and a document signature; and
   assembling a validation stamp for said signed document, wherein said validation stamp includes a validation signature and a validation body.

3. The method of claim 2 comprising the additional step of:

   appending said validation stamp to said signed document, wherein said validation stamp may be referenced to protect the integrity of said electronic signature on said electronic document.

4. The method of claim 2 or claim 3, wherein said document signature includes geometric information describing geometric signature features of a signator of said electronic signature.

5. The method of claim 4, wherein said geometric information is modified such that timing information corresponding to said geometric information cannot be reconstructed from modified geometric information.

6. A method for verifying the integrity of an electronic signature on an electronic document having a signed document and an encrypted validation stamp, said method comprising the steps of:

   decrypting said validation stamp; and

comparing said validation stamp being decrypted against said signed document to determine whether said electronic signature was originally intended by an authorized signator to be affixed to said electronic document.

7. The method of claim 6, wherein said signed document includes a document body and said validation stamp includes a validation body, said step of comparing said validation stamp includes:

comparing said validation body against said document body to determine whether said validation body coincides with said document body.

8. The method of claim 6 or claim 7, wherein said signed document includes said document signature and said validation stamp includes a validation signature, said method comprising the additional step of:

comparing timing information of said validation signature and geometric information of said document signature against geometric information and timing information of a signature known for an authorized signator to determine whether said electronic signature is a valid signature.

9. The method of claim 6 or 7, wherein said validation stamp includes a validation signature, said method comprising the additional step of:

comparing geometric information and timing information of said validation signature against geometric information and timing information of a signature known for an authorized signator to determine whether said electronic signature is a valid signature.

10. A method for verifying the integrity of an electronic signature on an electronic document having a signed document and an encrypted validation signature, said method comprising the steps of:

decrypting said validation signature; and
comparing said validation signature being decrypted against timing information of a signature known for an authorized signator of said signed document to determine whether said validation signature is a valid signature.

FIG. 1

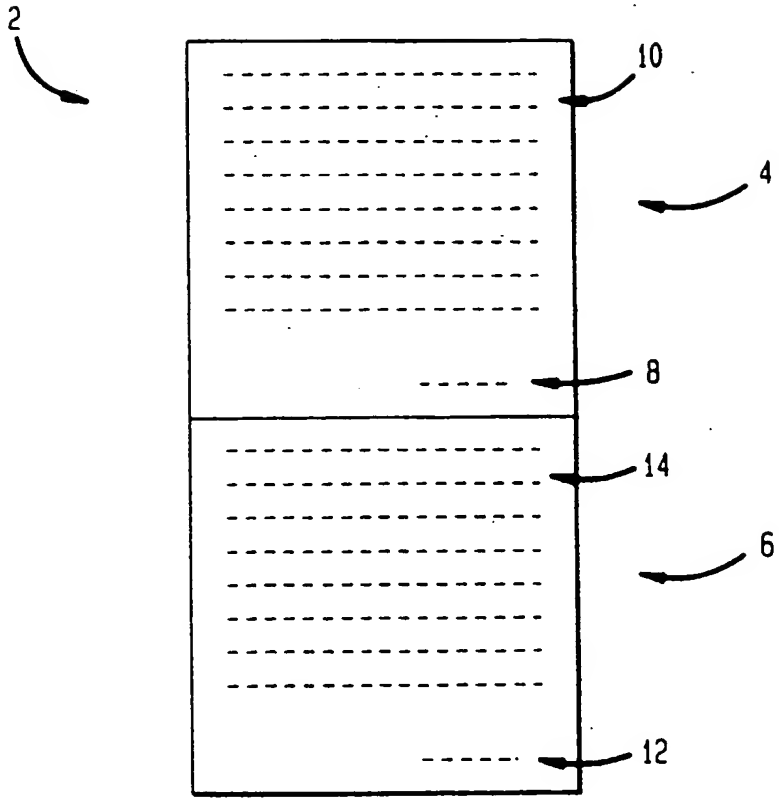

2
10
4
8
14
6
12

FIG. 4

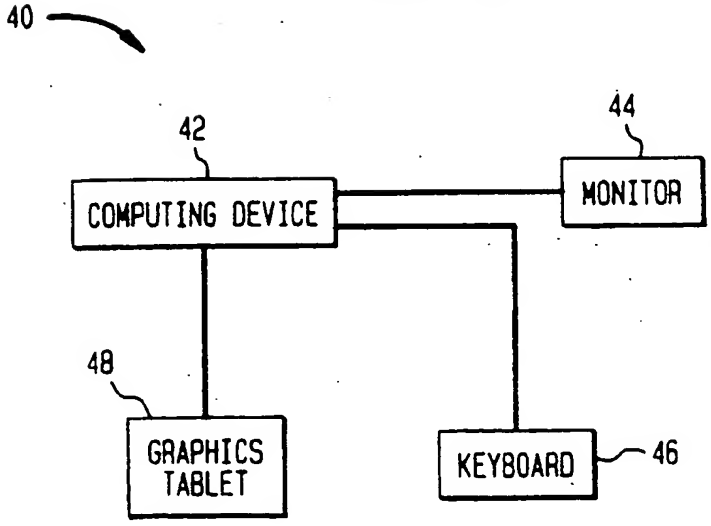
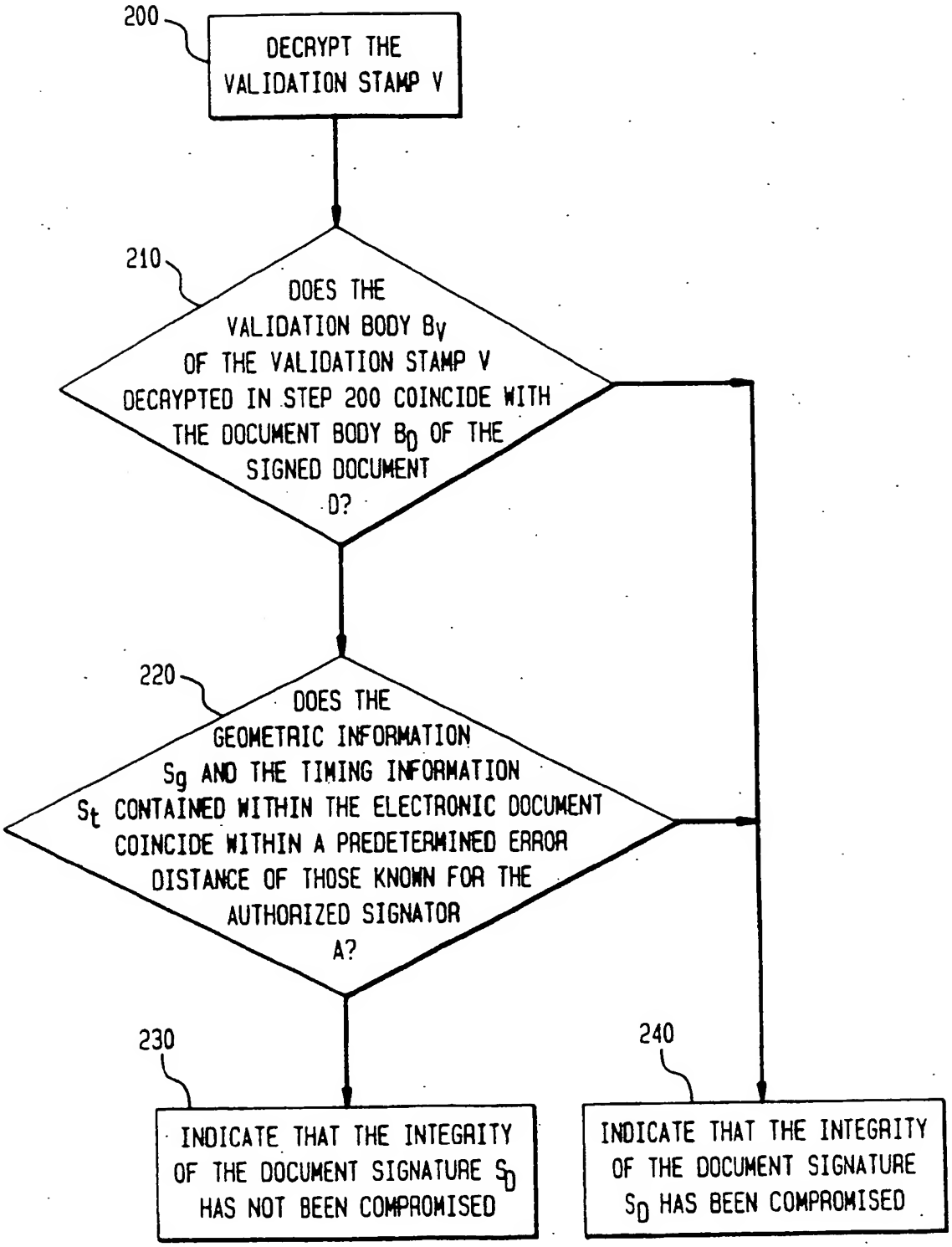

40
42
44
COMPUTING DEVICE
MONITOR
48
GRAPHICS TABLET
KEYBOARD
46

FIG. 2


200
DECRYPT THE VALIDATION STAMP V
210
DOES THE VALIDATION BODY B_V OF THE VALIDATION STAMP V DECRYPTED IN STEP 200 COINCIDE WITH THE DOCUMENT BODY B_D OF THE SIGNED DOCUMENT D?
220
DOES THE GEOMETRIC INFORMATION S_g AND THE TIMING INFORMATION S_t CONTAINED WITHIN THE ELECTRONIC DOCUMENT COINCIDE WITHIN A PREDETERMINED ERROR DISTANCE OF THOSE KNOWN FOR THE AUTHORIZED SIGNATOR A?
230
INDICATE THAT THE INTEGRITY OF THE DOCUMENT SIGNATURE S_D HAS NOT BEEN COMPROMISED
240
INDICATE THAT THE INTEGRITY OF THE DOCUMENT SIGNATURE S_D HAS BEEN COMPROMISED

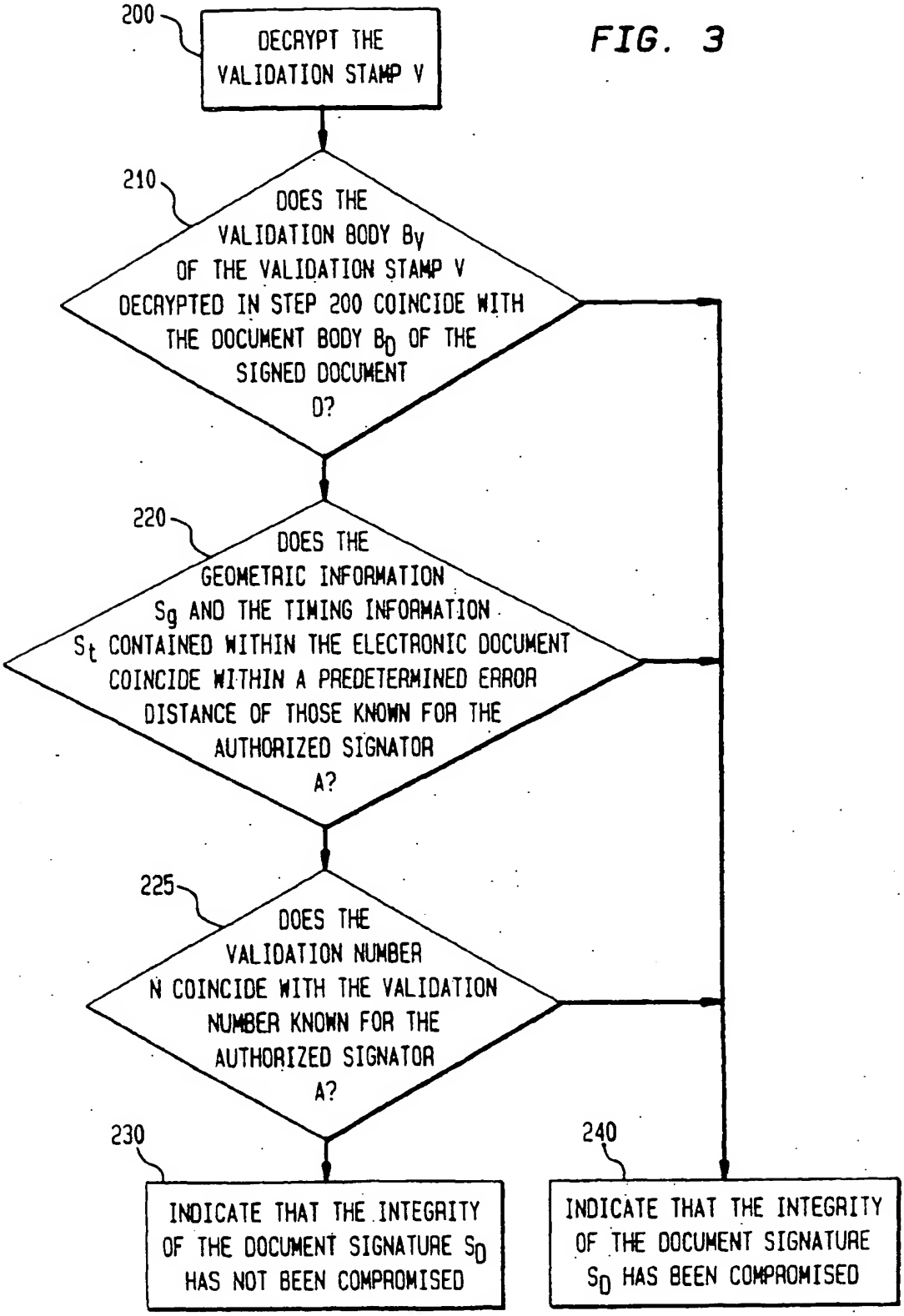

200
DECRYPT THE VALIDATION STAMP V
210
DOES THE VALIDATION BODY B_V OF THE VALIDATION STAMP V DECRYPTED IN STEP 200 COINCIDE WITH THE DOCUMENT BODY B_D OF THE SIGNED DOCUMENT D?
220
DOES THE GEOMETRIC INFORMATION S_g AND THE TIMING INFORMATION S_t CONTAINED WITHIN THE ELECTRONIC DOCUMENT COINCIDE WITHIN A PREDETERMINED ERROR DISTANCE OF THOSE KNOWN FOR THE AUTHORIZED SIGNATOR A?
225
DOES THE VALIDATION NUMBER N COINCIDE WITH THE VALIDATION NUMBER KNOWN FOR THE AUTHORIZED SIGNATOR A?
230
INDICATE THAT THE INTEGRITY OF THE DOCUMENT SIGNATURE S_D HAS NOT BEEN COMPROMISED
240
INDICATE THAT THE INTEGRITY OF THE DOCUMENT SIGNATURE S_D HAS BEEN COMPROMISED

FIG. 3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 97 30 6278

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	US 5 367 573 A (QUIMBY JOHN) * abstract; figure 3 *	2	H04N1/32 G06K9/00
Y	* column 1, line 31 - column 2, line 7 * * column 3, line 1 - line 13 *	3	
A	---	1,6	
X	US 5 208 858 A (VOLLERT EMMERAN ET AL) * column 2, line 3 - line 21 *	6	
A	---	1-3	
Y	DE 44 10 459 A (SIEMENS AG) * abstract; figure 1 *	3	
A	---	1,6,7	
A	US 5 157 726 A (MERKLE RALPH C ET AL) * abstract; figure 3 * * column 4, line 63 - column 5, line 32 *	1-3,6	
A	---	1,4	TECHNICAL FIELDS SEARCHED (Int.Cl.6)
	SATO Y ET AL: "ONLINE SIGNATURE VERIFICATION BASED ON SHAPE, MOTION, AND WRITING PRESSURE" PROCEEDINGS OF THE INTERNATIONAL JOINT CONFERENCE ON PATTERN RECOGNITION, MUNICH, OCTOBER 19- 22 1982. vol. 2, 19 October 1982, INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. pages 823-826, XP002011950 * the whole document * -----		H04N G06K G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	27 November 1997	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)